FTW
AF

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Docket No: SUNMP043C
GONG	Group Art Unit: 2137
Application No: 09/607,514	Examiner: Caldwell, Andy
Filed: June 28, 2000	Date: December 1, 2004
For: METHOD AND APPARATUS FOR SIGNING AND SEALING OBJECTS	

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on December 1, 2004.

Signed: _____
Neely J. Entwistle

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION -- 37 CFR 192)

Commissioner for Patents
Mail Stop: Appeal Brief- Patents
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is in furtherance of the Notice of Appeal filed in this case on September 27, 2004. The Notice of Appeal was received by the USPTO on October 1, 2004. Therefore, the due date for this Appeal Brief is December 1, 2004. This Appeal Brief is transmitted in triplicate:

This application is on behalf of:

☐ Small Entity ☒ Large Entity

Pursuant to 37 CFR 1.17(f), the fee for filing the Appeal Brief is:

☐ $170.00 (Small Entity) ☒ $340.00 (Large Entity)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136 apply:

☐ Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

Months	Large Entity	Small Entity
☐ one	$110.00	$55.00
☐ two	$430.00	$215.00
☐ three	$980.00	$490.00

☐ If an additional extension of time is required, please consider this a petition therefor.

☐ An extension for __ months has already been secured and the fee paid therefor of $ is deducted from the total fee due for the total months of extension now requested.

☒ Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that Applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Total Fees Due:

Notice of Appeal Fee	$340.00
Extension Fee (if any)	$_____
Total Fee Due	**$340.00**

☒ Enclosed is Check No. 12986 in the amount of $340.00.

☒ Charge any additional fees or credit any overpayment to Deposit Account No. 50-0850, (Order No. SUNMP043C). Two copies of this transmittal are enclosed.

Respectfully submitted,
MARTINE & PENILLA, LLP

Kenneth D. Wright
Registration No. 53,795

710 Lakeway Drive, Suite 200
Sunnyvale, CA 94085
(408) 749-6900
Customer No. 32291

Attorney Docket No.: SUNMP043C

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

EX PARTE GONG

Application for Patent

Filed June 28, 2000

Application No. 09/607,514

FOR:

METHOD AND APPARATUS FOR SIGNING AND SEALING OBJECTS

APPEAL BRIEF

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on December 1, 2004.
Signed:

Neely Entwistle

12/07/2004 HMARZI1 00000001 09607514
01 FC:1402 340.00 OP

MARTINE & PENILLA, LLP
Attorneys for Applicant

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is Sun Microsystems, Inc., the assignee of the present application.

II. RELATED APPEALS AND INTERFERENCES

The undersigned is not aware of any related appeals and/or interferences.

III. STATUS OF THE CLAIMS

A total of 31 claims were presented during prosecution of this application. The Applicant appeals rejected claims 1, 3-11, 13-25, and 29-31.

IV. STATUS OF THE AMENDMENTS

The application was originally filed on June 28, 2000, as a continuation application of U.S. Application No. 08/865,556, filed on May 29, 1997. All amendments have been entered, leaving rejected claims 1, 3-11, 13-25, and 29-31.

V. SUMMARY OF THE INVENTION

The present invention provides a method and an apparatus for signing and sealing objects. (p. 14, 1st ¶) In one embodiment, the present invention is used to sign an object such that it can be authenticated. (p. 15, last ¶) Embodiments of the present invention can also be used to encrypt an object, i.e., seal the object, to limit access to the object. (p. 15, last ¶) The signing and sealing mechanisms of the present invention can be combined to create a signed, sealed object. (p. 16, 1st partial ¶)

Object signing is a mechanism for creating a digitally signed version of an object that is unforgeable. (p. 16, 1st full ¶) A signed object can be passed within or between

runtime systems as a verifiable authentic token or object. (p. 16, 1st full ¶) Other applications can use the signed object internally to a runtime environment as an unforgeable authorization token that can be passed around without concern regarding malicious, undetected modification of the signed object. (p. 16, 1st full ¶) Also, a signed object can be stored outside the runtime environment, e.g., on a disk, to serve as critical access control data. (p. 16, 1st full ¶)

In the present invention, a signedObject class is defined to sign an object. (p. 16, last ¶) Figure AB-1 (Figure 2) is an illustration showing an overview of a signedObject class, in accordance with one embodiment of the present invention. The signedObject class 202 is used to sign object 204 that is instantiated in a runtime environment. (p. 16, last ¶) A snapshot of object 204 is created and stored in array 214. (p. 16, last ¶) The snapshot includes the state of object 204. (p. 16, last ¶) For example, the snapshot includes a class of object 204, a class signature, and values of all non-transient and non-static fields of object 204. (p. 16, last ¶) A signature is generated by signature generator 206 and is stored in array 216 of signedObject 202. (p. 16, last ¶)

Arrays 214 and 216 are publicly accessible via methods of signedObject 202. (p. 17, 1st ¶) For example, signedObject 202 can limit access such that a request to modify array 214 is not allowed when a valid signature exists in array 216. (p. 17, 1st ¶) Alternatively, a request to modify array 214 can be allowed; however, the valid signature in array 216 is invalidated as a result. (p. 17, 1st ¶) Another method of signedObject 202 provides the ability to examine the status of array 216 (i.e., whether array 216 contains a valid signature). (p. 17, 1st ¶) The contents of arrays 214 and 216 can be retrieved using methods of signedObject 202. (p. 17, 1st ¶)

The snapshot of object 204 stored in array 214 can be used to reconstruct object 204. (p. 17, 2nd ¶) The signature contained in array 216 is examined to verify authenticity

(i.e., that the object originates from a trusted source). (p. 17, 2nd ¶) If the signature is authentic, the contents of array 214 are used to reconstruct object 204. (p. 17, 2nd ¶) For example, the contents of array 214 can contain the state of object 204 which is used to populate the fields of an instance of object 204. (p. 17, 2nd ¶) Alternatively, array 214 can include both the state and the behavior of object 204. (p. 17, 2nd ¶)

In addition to the signedObject class, the present invention also defines a sealedObject class for sealing an object. (p. 17, last ¶) Figure AB-2 (Figure 3) is an illustration showing an overview of a sealedObject class, in accordance with one embodiment of the present invention. (p. 17, last ¶) In one embodiment, the sealedObject class is a subclass of the signedObject class. (p. 17, last ¶) Thus, the sealedObject class inherits member fields and methods of the signedObject class. (p. 18, 1st partial ¶) With respect to Figure AB-2, a sealedObject 202 is used to seal object 204 by encrypting the contents of object 204. (p. 18, 1st partial ¶) A snapshot of object 204 is created and stored in array 214. (p. 18, 1st partial ¶) The snapshot includes the state of object 204. (p. 18, 1st partial ¶) For example, the snapshot includes the class of object 204, the class signature, and values of all non-transient and non-static fields of object 204. (p. 18, 1st partial ¶) A signature is generated by signature generator 206 and is stored in array 216 of signedObject 202. (p. 18, 1st partial ¶)

Arrays 214 and 216 are accessible via methods of signedObject 202. (p. 18, 1st full ¶) As a subclass of signedObject 202, sealedObject 302 includes the methods of signedObject 202 for modifying array 214, examining the status of array 216 (i.e., whether array 216 contains a valid signature), retrieving the contents of arrays 214 and 216, etc. (p. 18, 1st full ¶) An instance of sealedObject 302 further includes methods for encrypting and decrypting a snapshot of object 204. (p. 18, 1st full ¶) Other methods of sealedObject 302

provide an ability to determine a status of sealedObject 302 and retrieve content of array 318. (p. 18, 1st full ¶)

Array 318 includes an encrypted version, i.e., ciphertext, for the snapshot of object 204. (p. 18, last ¶) To encrypt object 204, a snapshot of object 204 is generated and stored in array 214. (p. 18, last ¶) Encryptor 308 is used to encrypt the contents of array 214 using an encryption key. (p. 18, last ¶) In one embodiment, a public key system is used to sign or seal an object. (p. 18, last ¶) The encrypted snapshot is stored in array 318. (p. 19, 1st partial ¶) The content of array 214 is then deleted such that a plaintext version of the snapshot is no longer stored in sealedObject 302. (p. 19, 1st partial ¶) Thus, once a ciphertext version of object 204 is generated, the plaintext version of object 204 is deleted from sealedObject 302. (p. 19, 1st partial ¶)

When signing or sealing an object as previously described, the present invention provides for taking a snapshot of the object using a process referred to as serialization. (p. 21, 1st ¶) During serialization the content of the object is retrieved from the object and saved in, for example, a file, a byte array, etc. (p. 21, 1st ¶) Additionally, the present invention provides for restoring the content of an object using a process of deserialization. (p. 21, 1st ¶) In one embodiment, streaming is used to serialize and deserialize an object. (p. 21, 1st ¶)

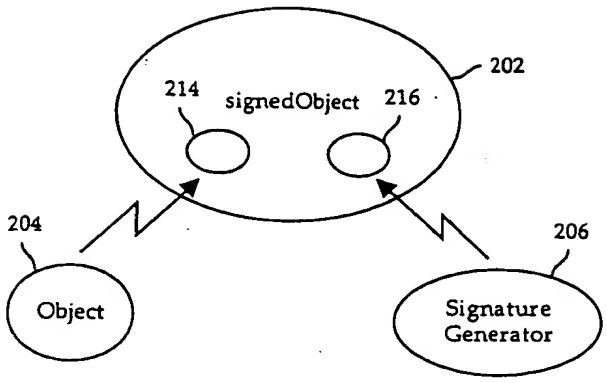

Figure AB-1

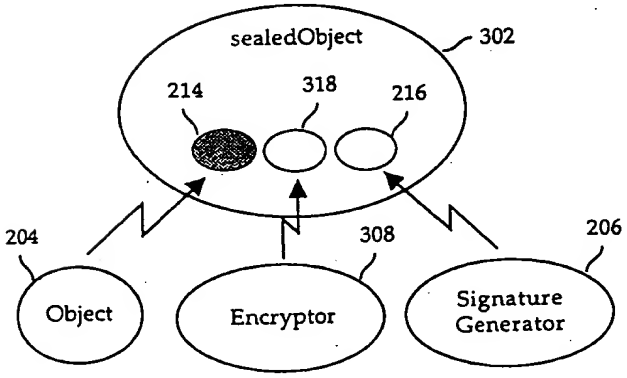

Figure AB-2

VI. ISSUES

The issues presented in this appeal are whether the rejections under 35 U.S.C. §103 of the claims under appeal are proper. The issues therefore are as follows:

A. Are claims 1, 3-7, 11, 13-17, and 29 properly rejected under 35 U.S.C. §103(a) as being unpatentable over Griffin (U.S. Patent No. 5,893,077) in view of Schneier (*Applied Cryptography*)?

B. Are claims 8-10, 18-21, and 30-31 properly rejected under 35 U.S.C. §103(a) as being unpatentable over Griffin and Schneier in further view of Chaplin (U.S. Patent No. 5,315,655)?

C. Are claims 22-25 properly rejected under 35 U.S.C. §103(a) as being unpatentable over Griffin in view of Schneier in view of Fischer (U.S. Patent No. 5,390,247) and further in view of Chaplin?

VII. GROUPING OF THE CLAIMS

The applicant proposes three groups of claims. The first group (Group I) includes claims 1, 3-11, and 13-25. The claims of the first group stand or fall together. The second group (Group II) includes claim 29. The third group (Group III) includes claims 30-31. The claims of the third group stand or fall together.

VIII. ARGUMENTS

A. The references as relied upon by the Examiner, either separately or in combination, do not motivate or suggest to one of ordinary skill in the art at the time of the invention to combine the reference teachings in a manner that would render the invention as recited in claims 1, 3-11, and 13-25 (Group I) prima facie obvious.

Rejection

Claims 1, 3-7, 11, and 13-17 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Griffin in view of Schneier. Claims 8-10 and 18-21 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Griffin and Schneier in further view of

Chaplin. Claims 22-25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Griffin in view of Schneier in view of Fischer and further in view of Chaplin. These rejections are traversed.

Examiner's Position

With regard to claim 1, the Examiner's position is as follows:

> "It would have been obvious to a person of ordinary skill in the art at the time the invention was made to use the serialized object of Griffin to generate the signature so that the signature could be used as a proof against the object."

Applicant's Rebuttal

Claim 1 represents the broadest independent claim of Group I (i.e., claims 1, 3-11, and 13-25). Since the claims of Group I will stand or fall together, the Applicant chooses to argue the patentability of claim 1. Therefore, the arguments presented in this section (Section VIII.A.) are directed to claim 1.

The Examiner has relied upon Griffin to teach taking a snapshot of a live object by serializing a state of the live object. The Examiner has also relied upon Griffin to teach constructing a new object using the snapshot of the live object. The Examiner has relied upon Schneier to teach associating a signature with the snapshot of the live object having been taken by serializing the state of the live object. The Examiner has also relied upon Schneier to teach verifying the signature associated with snapshot of the live object to enable construction of the new object using the snapshot of the live object. For reasons discussed in Section VIII.B., the Applicant submits that Griffin and Schneier do not teach the features of claim 1 as asserted by the Examiner. Additionally, the Applicant submits that there is no motivation or suggestion to combine the teachings of Griffin and Schneier as suggested by the Examiner.

The disclosures of Griffin and Schneier do not have any commonality that would suggest combining their respective teachings to arrive at the present invention as suggested by the Examiner. Griffin does not include any reference or suggestion to generation of a signature, association of a signature with an entity, or verification of a signature for a particular purpose. Additionally, the Examiner has admitted that "Griffin does not say that a signature is associated with the serialized object or that the association between the two is maintained." While Schneier does include teachings associated with signatures, Schneier does not include any suggestion to apply the signatures in the manner required by claim 1. More specifically, Schneier does not suggest maintaining an association between a signature and a snapshot of the live object, wherein the snapshot of the live object has been previously taken by serializing a state of the live object. Schneier also does not suggest verifying the signature associated with the snapshot to enable construction of a new object using the snapshot of the live object.

In view of the foregoing, the Applicant submits that Griffin does not include any teaching that would lead one of ordinary skill in the art to look to Schneier when creating the present invention as recited in claim 1, vice-versa. Therefore, for at least the reasons provided above, the Applicant submits that there is no suggestion or motivation, either explicitly or implicitly, in either Griffin or Schneier to have combined their respective teachings to arrive at the present invention as embodied in claim 1. Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either explicitly or implicitly in the references themselves or in the knowledge generally available to one of ordinary skill in the art. MPEP §2143.01 However, the level of ordinary skill in the art cannot be relied upon to provide the suggestion to combine references. *Al-Site Corp. v. VSI Int'l Inc.*, 174 F.3d 1308, 50 USPQ2d 1161 (Fed. Cir. 1999).

A statement that modifications of the prior art to meet the claimed invention would have been within the ordinary skill of the art at the time the claimed invention was made is not sufficient to establish a prima facie case of obviousness without some objective reason to combine the teachings of the references. *Ex parte Levengood*, 28 USPQ2d 1300 (Bd. Pat. App. & Inter. 1993). Simply asserting that one of ordinary skill in the art at the time of the invention may have been inclined to combine the teachings of the references is not an objective reason for combining the teaching of the references. Additionally, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990).

In view of the foregoing, the Board of Appeals and Interferences ("Board" hereafter) is respectfully requested to overrule the Examiner's rejections of claims 1, 3-11, and 13-25 under 35 U.S.C. §103.

B. The combination of Griffin, Schneier, and Chaplin, as relied upon by the Examiner, fail to teach or suggest all features recited in each of claims 1, 3-11, and 13-25 (Group I) as required to establish a prima facie case of obviousness.

Rejection

Claims 1, 3-7, 11, and 13-17 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Griffin in view of Schneier. Claims 8-10 and 18-21 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Griffin and Schneier in further view of Chaplin. Claims 22-25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Griffin in view of Schneier in view of Fischer and further in view of Chaplin. These rejections are traversed.

Examiner's Position

With regard to claim 1, the Examiner's position is as follows:

"In figure 9, Griffin shows the serialization of an object (element 387). This meets the limitation of taking a snapshot by serializing the state of a live object. The object has necessarily been instantiated in a runtime environment. Griffin does not say that a signature is associated with the serialized object or that the association between the two is maintained. On page 39, Schneier shows a digital signature that is made by encrypting a message-to-be-authenticated with a private key. Decryption using the corresponding public key not only retrieves the data, but also indicates that the data was encrypted by the private key's holder. Schneier's signature method includes verification. Deserialization, shown in element 508 of figure 11A in Griffin, meets the limitation of constructing a new object using said snapshot. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use the serialized object of Griffin to generate the signature so that the signature could be used as a proof against the object."

Applicant's Rebuttal

Claim 1 represents the broadest independent claim of Group I (i.e., claims 1, 3-11, and 13-25). Since the claims of Group I will stand or fall together, the Applicant chooses to argue the patentability of claim 1. Therefore, the arguments presented in this section (Section VIII.B.) are directed to claim 1.

The Examiner has relied upon Griffin to disclose each required feature of claim 1 with the exception of the signature features. In addition, the Examiner has relied upon Schneier to disclose the signature features of claim 1. In order to respond to the combination of Griffin and Schneier as applied by the Examiner, it is necessary for the Applicant to address each feature of the presently claimed invention on an individual basis with respect to the specific cited art that is being applied against the particular feature.

Therefore, the Applicant respectfully submits that the following arguments should not be viewed as attacking references individually.

Griffin discloses an event generation and collection system for a distributed network that includes an event source for generating event objects and an event collector for gathering event objects. Griffin discloses that each event object is serialized to create a binary representation of the event object in a memory buffer. Then, according to Griffin, conversion routines are run on the event object data so that the data can be converted to a format useful to other processes in the distributed network.

Griffin further discloses that once event objects are gathered and serialized, the event objects are stored together in an event object file. Griffin also discloses that event object files are transmitted across the distributed network, rather than distributing the individual event objects contained therein. Griffin further discloses that when an event object file is retrieved, the event object file is converted to an export format file which is then imported into a database server. The database server then accesses the export format file and retrieves data of interest to a process operating on the database server. It should be understood that Griffin does not disclose using the serialized event object data to recreate the event object.

The Examiner has relied upon Schneier to disclose signature and encryption methods for digital data. The Examiner has asserted that the combination of Griffin and Schneier disclose each and every feature of claim 1, including constructing a new object using said snapshot. The Applicant respectfully submits that neither Griffin, Schneier, nor the combination thereof disclose each and every feature of claim 1. In particular, neither Griffin, Schneier, nor the combination thereof disclose constructing a new object using said snapshot, wherein said snapshot refers to a snapshot taken of a live object by serializing a state of the live object.

The disclosure of Schneier is silent with regard to taking a snapshot of a live object by serializing a state of the live object. Also, the disclosure of Schneier is silent on constructing a new object using the snapshot of the live object. Furthermore, it should be understood that Schneier is only referenced by the Examiner to address generating a signature for digital data. Therefore, with respect to the Schneier/Griffin combination, it should be understood that Schneier provides no contribution with respect to disclosing or suggesting construction of a new object using a snapshot taken of a live object.

As with Schneier, the disclosure of Griffin is silent with regard to constructing a new object using a snapshot taken of a live object. Griffin discloses that event object data is serialized. Griffin also discloses that the serialized event object data is stored in an event object file. Griffin then states that the event object file is used as a vehicle for transmitting the event object data over a network. With respect to Griffin, Figure 12, a process is described in which the event object file is converted to an export format file, which is in turn imported into a database server. Griffin then discloses how the database server accesses the export format file to retrieve event object data for further processing by the database server. Griffin does not discuss the further processing by the database server. In particular, Griffin does not discuss or suggest using the serialized event object data for the purpose of recreating an event object. Therefore, Griffin does not disclose or suggest constructing a new object using a snapshot taken of a live object, as required by claim 1.

The Examiner has asserted that "Deserialization, shown in element 508 of Figure 11A in Griffin, meets the limitation of constructing a new object using said snapshot." The Applicant disagrees with this assertion by the Examiner. Simply stated, de-serialization is not equivalent to constructing a new object. Griffin as previously discussed, discloses de-serialization of event object data, but the de-serialization of Griffin does not result in the

construction of a new event object. As demonstrated by Griffin, the process of de-serializing serialized data is not sufficient to suggest construction of a new object.

In view of the foregoing, the combination of Schneier and Griffin fails to disclose constructing a new object using a snapshot taken of a live object as required by claim 1. To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). In accordance with foregoing arguments, the Applicant respectfully submits that the combination of Griffin and Schneier fails to teach or suggest each and every feature of claim 1 as required to support a rejection under 35 U.S.C. §103(a). Therefore, the Applicant submits that claim 1 is patentable over the cited art of record.

In view of the foregoing, the Board is respectfully requested to overrule the Examiner's rejections of claims 1, 3-11, and 13-25 under 35 U.S.C. §103.

C. The combination of Griffin and Schneier, as relied upon by the Examiner, fail to teach or suggest all features recited in claim 29 (Group II) as required to establish a prima facie case of obviousness.

Rejection

Claim 29 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Griffin in view of Schneier. This rejection is traversed.

Examiner's Position

Since the Examiner's Position with respect to claim 29 is essentially the same as that with respect to claim 1, the Board is respectfully requested to refer to the Examiner's Position with respect to claim 1 as provided in Section VIII.B. Additionally, with respect to claim 29, the Examiner has stated that "arrays are fundamental to structured data" and that the "event object file [of Griffin] is structured data."

Applicant's Rebuttal

The Examiner has applied the combination of Griffin and Schneier against claim 29 in the same manner as applied against claim 1. Therefore, with respect to features of claim 29 that are similar to features of claim 1, the Applicant submits that the arguments presented in the Applicant's Rebuttal of Section VIII.B are equally applicable to claim 29. Thus, in the interest of minimizing repetitive discussion, the Board is respectfully requested to refer to Section VIII.B for at least a portion of the Applicant's Rebuttal to the Examiner's Position of the present section.

In addition to the foregoing, it should be noted that claim 29 requires instantiating the signed object to create a snapshot array and a signature array associated with the signed object. Also, claim 29 requires the captured state of the live object to be stored in the snapshot array and the associated signature to be stored in the signature array. The Examiner has asserted that arrays are fundamental to structured data. Also, the Examiner has asserted that the event object file (of Griffin) is structured data. The Examiner has not provided any further explanation of how Griffin or any other cited art of record discloses or suggests instantiating a signed object to create a snapshot array and a signature array associated with the signed object. The Examiner also has not specifically indicated how the cited art of record suggests storing a captured state of a live object in a snapshot array and an associated signature in a signature array. The Applicant submits that the Examiner has not properly considered all words of claim 29 in judging the patentability of claim 29 against the cited art of record. All words in a claim must be considered in judging the patentability of that claim against the prior art. *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

In view of the foregoing, the Examiner has not demonstrated how each and every feature of claim 29 is disclosed or suggested by the cited art of record. To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or

suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). In accordance with foregoing arguments, the Applicant respectfully submits that the combination of Griffin and Schneier fails to teach or suggest each and every feature of claim 29 as required to support a rejection under 35 U.S.C. §103(a). Therefore, the Applicant submits that claim 29 is patentable over the cited art of record.

In view of the foregoing, the Board is respectfully requested to overrule the Examiner's rejection of claim 29 under 35 U.S.C. §103.

D. The combination of Griffin, Schneier, and Chaplin as relied upon by the Examiner, fail to teach or suggest all features recited in claims 30-31 (Group III) as required to establish a prima facie case of obviousness.

Rejection

Claims 30-31 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Griffin and Schneier in further view of Chaplin. These rejections are traversed.

Examiner's Position

The Examiner states that claims 30-31 are rejected over Griffin and Schneier as applied to claim 1 and further in view of Chaplin.

Therefore, the Board is respectfully requested to refer to the Examiner's Position with respect to claim 1 as provided in Section VIII.B. Additionally, with respect to Chaplin, the Examiner states that "Figure 7 of Chaplin clearly shows the encryption of data in part 704 and then the deletion of the unencrypted copy of the data in part 705." The Examiner further states that "Chaplin also teaches decryption of data in figure 8."

Applicant's Rebuttal

The Examiner has applied the combination of Griffin and Schneier against claim 30 in the same manner as applied against claim 1. Therefore, with respect to features of claim 30 that are similar to features of claim 1, the Applicant submits that the arguments presented in the Applicant's Rebuttal of Section VIII.B are equally applicable to claim 30.

Thus, in the interest of minimizing repetitive discussion, the Board is respectfully requested to refer to Section VIII.B for at least a portion of the Applicant's Rebuttal to the Examiner's Position of the present section.

In addition to the foregoing, it should be noted that claim 30 requires instantiating the sealed object to create a snapshot array, a signature array, and an encryption array. Also, claim 30 requires the captured state of the live object to be stored in the snapshot array. Claim 30 further requires the encrypted version of the captured state of the live object to be stored in the encryption array.

The Examiner has asserted that arrays are fundamental to structured data. Also, the Examiner has asserted that the event object file (of Griffin) is structured data. The Examiner has not provided any further explanation of how Griffin, Schneier, or Chaplin discloses or suggests instantiating a signed object to create a snapshot array and a signature array associated with the signed object. The Examiner also has not specifically indicated how the cited art of record suggests storing a captured state of a live object in a snapshot array and an associated signature in a signature array. Furthermore, the Examiner has not specifically indicated how the cited art of record suggests storing an encrypted version of a captured state of a live object in an encryption array. The Applicant submits that the Examiner has not properly considered all words of claim 30 in judging the patentability of claim 30 against the cited art of record. All words in a claim must be considered in judging the patentability of that claim against the prior art. *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

In view of the foregoing, the Examiner has not demonstrated how each and every feature of claim 30 is disclosed or suggested by the cited art of record. To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). In

accordance with foregoing arguments, the Applicant respectfully submits that the combination of Griffin and Schneier fails to teach or suggest each and every feature of claim 30 as required to support a rejection under 35 U.S.C. §103(a). Therefore, the Applicant submits that claim 30 is patentable over the cited art of record.

In view of the foregoing, the Board is respectfully requested to overrule the Examiner's rejections of claims 30-31 under 35 U.S.C. §103.

E. Conclusion

In view of the inappropriateness of the 35 U.S.C. §103 rejections, as discussed in the Applicant's aforementioned arguments, the Applicant submits that the presently claimed invention is patentable over the cited art of record.

The Applicant respectfully requests the Board to consider each group of claims (Groups I, II, and III) separately with respect to the teachings of the cited art of record.

In summary, the Applicant submits that the Examiner's rejections are in error, and respectfully requests that the Board of Appeals and Interferences reverse the Examiner's rejections of the claims on appeal.

Respectfully Submitted,
MARTINE & PENILLA, LLP

Kenneth D. Wright
Reg. No. 53,795

MARTINE & PENILLA, LLP
710 Lakeway Drive, Suite 200
Sunnyvale, California 94085
408.749.6900

APPENDIX A

CLAIMS ON APPEAL

1. A method for signing a live object comprising:

instantiating a live object in a runtime environment;

taking a snapshot of said live object, wherein said taking said snapshot is performed by serializing a state of said live object;

associating a signature with said snapshot;

maintaining said association between said snapshot and said signature;

verifying said signature; and

constructing a new object using said snapshot, when said signature is verified.

3. The method of claim 1 further comprising:

storing said snapshot in another object; and

storing said signature in said another object.

4. The method of claim 1 further comprising:

monitoring a status of said snapshot; and

invalidating said signature when said status of said snapshot changes.

5. The method of claim 1 further comprising:

creating said signature using said snapshot.

6. The method of claim 5 further comprising:

associating a second signature with said snapshot.

7. The method of claim 6 further comprising:

verifying said second signature; and

constructing a new object using said snapshot, when said second signature is verified.

8. The method of claim 1 further comprising:

generating an encryption key;

generating an encrypted snapshot of said snapshot;

deleting said snapshot; and

associating said signature with said encrypted snapshot, said signature previously being associated with said snapshot.

9. The method of claim 8 further comprising:

maintaining said association between said encrypted snapshot and said signature associated with said encrypted snapshot.

10. The method of claim 9 further comprising:

verifying said signature associated with said encrypted snapshot; and

constructing a new object using encrypted said snapshot, when said signature associated with said encrypted snapshot is verified.

11. A computer program product for signing a live object comprising a computer readable medium having recorded thereon:

computer program code for causing a computer to instantiate a live object in a runtime environment;

computer program code for causing a computer to take a snapshot of said live object by serializing a state of said live object;

computer program code for causing a computer to associate a signature with said snapshot;

computer program code for causing a computer to maintain said association between said snapshot and said signature;

computer program code for causing a computer to verify said signature; and

computer program code for causing a computer to construct a new object using said snapshot, when said signature is verified.

13. The computer program product of claim 11 further comprising:

computer program code for causing a computer to store said snapshot in another object; and

computer program code for causing a computer to store said signature in said another object.

14. The computer program product of claim 11 further comprising:

computer program code for causing a computer to monitor a status of said snapshot;

computer program code for causing a computer to invalidate said signature when said status of said snapshot changes.

15. The computer program product of claim 11 further comprising:

computer program code for causing a computer to create said signature using said snapshot.

16. The computer program product of claim 11 further comprising:

computer program code for causing a computer to associate a second signature with said snapshot.

17. The computer program product of claim 16 further comprising:

computer program code for causing a computer to verify said second signature; and

computer program code for causing a computer to construct a new object using said snapshot, when said second signature is verified.

18. The computer program product of claim 11 further comprising:

computer program code for causing a computer to generate an encryption key;

computer program code for causing a computer to encrypt said snapshot;

computer program code for causing a computer to delete said snapshot ; and

computer program code for causing a computer to associate said signature with said encrypted snapshot, said signature previously being associated with said snapshot.

19. The computer program product of claim 18 further comprising:

computer program code for causing a computer to decrypt said encrypted snapshot.

20. The computer program product of claim 18 further comprising:

computer program code for causing a computer to maintain said association between said encrypted snapshot and said signature associated with said encrypted snapshot.

21. The computer program product of claim 20 further comprising:

computer program code for causing a computer to verify said signature associated with said encrypted snapshot; and

computer program code for causing a computer to construct a new object using said encrypted snapshot, when said signature associated with said encrypted snapshot is verified.

22. A system configured to sign a live object existing in a runtime environment, said system comprising:

a first module of program code executing on a computer configured to take a snapshot of a live object, wherein said snapshot is a serialization of a state of said live object;

a second module of program code executing on said computer configured to generate a signature using said snapshot, said first module configured to monitor a status of said snapshot, and to invalidate said signature when said snapshot is changed; and

a sealing module including,

a key generation module configured to generate an encryption key,

an encryption module configured to generate an encrypted snapshot from said snapshot, and

a deletion module configured to delete said snapshot,

wherein said second module is configured to invoke said key generation module, said encryption module, and said deletion module,

wherein said second object is configured to verify said signature and construct a new object using said encrypted snapshot when said signature is verified.

23. The system of claim 22 wherein said first and second modules are implemented as a second object.

24. The system of claim 23 wherein said snapshot and said signature are stored in said second object, said second object limiting access to said snapshot through one or more methods of said second object.

25. The system of claim 24 wherein said one or more methods of said second object invalidate said signature when said access modifies said snapshot.

29. A method for creating a signed object representing a state of a live object presently instantiated in a runtime environment, the live object containing dynamic data, comprising:

instantiating the signed object, wherein the instantiating creates a snapshot array and a signature array associated with the signed object;

invoking a method of the signed object to capture the state of the live object, wherein the state of the live object includes one or more current values for the dynamic data;

storing the captured state of the live object in the snapshot array;

generating a signature associated with the captured state of the live object stored in the snapshot array; and

storing the signature in the signature array.

30. A method for creating a sealed object representing an encrypted version of a state of a live object presently instantiated in a runtime environment, the live object containing dynamic data, comprising:

instantiating the sealed object, wherein the instantiating creates a snapshot array, a signature array, and an encryption array associated with the sealed object;

invoking a first method of the sealed object to capture the state of the live object, wherein the state of the live object includes one or more current values for the dynamic data;

storing the captured state of the live object in the snapshot array;

invoking a second method of the sealed object to create an encrypted version of the captured state of the live object stored in the snapshot array;

storing the encrypted version of the captured state of the live object in the encryption array; and

removing the captured state of the live object from the snapshot array.

31. The method of claim 30, further comprising:

generating a signature associated with the captured state of the live object stored in the snapshot array, wherein the generating is performed prior to invoking the second method of the sealed object; and

storing the signature in the signature array.